In the drawings:

Please replace the drawings with the formalized drawings provided in the replacement sheets at the end of this response. The replacement drawings are to provide drawings that are professionally rendered for better appearance.

REMARKS

Reconsideration is respectfully requested. Claims 1 and 2 are present in the application. Claims 3 and 4 are newly added.

Support for claims 3 and 4 is found in the specification as filed. The network test instrument 50 is shown in FIG. 1. The operational steps thereof are discussed in the specification pages 3-5 and in FIG. 2.

The drawings are objected to because items 118 and 120 from Fig. 2 are not mentioned in the specification. The specification is amended herein to put reference to these drawings in the respective locations. This is not new matter as the text clearly recites the steps that are set forth in the drawing blocks 118 and 120 and the reference to the specific blocks in FIG. 2 was merely inadvertently not typed in when the specification was written.

Claims 1 and 2 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Haneda (US 2002/0167914A1) in view of Bearden et al (US 2003/0086425A1).

Applicant respectfully traverses.

Neither Haneda nor Bearden et al mention the term uplink bridge, nor even the word uplink.

The action states that Bearden et al teaches in paragraph [0150] the concept of "for any interface index retrieved from

said selected bridge, identifying a port associated with said interface index as an uplink port of an adjacent bridge."

Applicant disagrees.

Paragraph [0150] of Bearden et al states:

> Next the topology analysis algorithm identifies the layer 2 links in the network, as follows. Recall that each layer 2 link is identified by a pair of device identifiers, say D_i and D_j, and by a particular interface on each of the devices, say $I_{i,m}$ and $I_{j,n}$. The algorithm iterates (482) through the spanning tree table entries of all layer-2 switching devices in the network. For each entry in the spanning tree table of a device D_i, that identifies for port $P_{i,m}$, the designated bridge is D_j and the designated port is $P_{j,n}$, the algorithm processes the entry as follows: If the designated switch D_j in the entry is the same as Di then the entry is skipped (483). Otherwise the entry indicates there is a layer-2 link between D_i and D_j using ports $P_{i,m}$ and $P_{j.n}$ (484). The port numbers $P_{i,m}$ and $P_{j.n}$ thus identified are mapped to the interface IDs of the link by locating the dotldStpPortTable MIB entry at each device that matches each the device's port number. That is to say, the entries for ports $P_{i,m}$ and $P_{j,n}$ in the dotldStpPortTable MIBs of D_i and D_j, respectively, provide the ifIndex (485) values $I_{i,m}$ and $I_{j,n}$ that are recorded by the algorithm to identify the particular layer 2 link from D_i to D_j. Each entry is processed in this same manner until all of the layer-2 links are identified. The set of identified links, along with the layer 2 devices already identified earlier, comprise the output of the layer-2 topology analysis algorithm.

There is no mention of uplink port of an adjacent bridge. Nowhere in Bearden et al does the term "uplink" appear.

It is respectfully submitted that Bearden et al and Haneda, whether considered alone or when combined, do not teach or

suggest claim 1. It is submitted that the documents do not appreciate the applicant's claims and are silent as to the issue being addressed by applicant's claims.

Further, with respect to claim 2, the office action states that Bearden et al discusses counting a number of MAC addresses associated with each port of said bridges in paragraphs 0107-0108. Applicant respectfully traverses.

Paragraphs 107 and 108 of Bearden et al do not mention counting the number of MAC addresses associated with each port of a bridge. Paragraphs 107 and 108 of Bearden et al, reproduced below (emphasis added by applicant's representative), make no mention of counting MAC addresses associated with each port.

> [0107] The second step, alias detection, (452) identifies cases where one device responded to multiple addresses (i.e., the address is aliased). It is common for devices (e.g., routers) to be assigned multiple addresses. Since we are interested in a list of devices, rather than a list of addresses, it is advantageous to identify which addresses belong to the same device. Given that we can identify when a single device responded to multiple addresses, <u>this step marks the repeated addresses such that the subsequent steps will only use one of the device's addresses</u>.
>
> [0108] An example of how this can be done is as follows. Certain data, such as physical addresses (e.g. MAC addresses), are assigned uniquely to devices and are readily available via SNMP (the standard interfaces MIB contains the physical address used for each interface on the device). Thus, if a device responded to multiple addresses, the

> interface tables collected from each of its addresses would have the same physical addresses, and interface tables collected from addresses used by distinct devices would have different physical addresses.

These portions of Bearden et al merely mention that if multiple addresses are found, they are marked. There is no concept of counting them and of identifying a port as an uplink port if the count exceeds a predetermined number. In fact, Bearden et al want to avoid dealing further with the multiple addresses (see underlined portion above) and mark them so that subsequent steps only use a single address. There is no discussion of counting them, only marking them to avoid using them in the future steps. Such marking does not meet the counting concept of applicant's claim.

Further, it is stated in the office action that Bearden et al show in paragraphs [0018], [0019] and [0150] the step of identifying a port as an uplink port if said number of MAC addresses counted exceeds a predetermined number. Applicant respectfully disagrees. Bearden et al teach no such concept in these paragraphs set forth below:

> [0118] Network administrators may use access control mechanisms to protect against unwanted access. For example, the SNMP protocol (SNMPv1 and SNMPv2) uses a concept called a community string to provide access control. A device only responds to requests that use a community string that it is configured to use. Network administrators provide protection against unauthorized access by configuring the devices to use a non-standard community string. In this

context, the system administrators can provide the user with any non-standard community strings used in the network.

[0119] In the case where non-standard or multiple access control parameters (e.g., community strings) are used, a slight modification of the steps above are needed. In step 451, the probe must be repeated for each control parameter. When a device responds, the system must record which control parameters were used for that device. In the remaining steps, when requesting data from a device, an appropriate set of parameters needs to be used.

[0150] Next the topology analysis algorithm identifies the layer 2 links in the network, as follows. Recall that each layer 2 link is identified by a pair of device identifiers, say D_i and D_j, and by a particular interface on each of the devices, say $I_{i,m}$ and $I_{j,n}$. The algorithm iterates (482) through the spanning tree table entries of all layer-2 switching devices in the network. For each entry in the spanning tree table of a device D_i, that identifies for port $P_{i,m}$, the designated bridge is D_j and the designated port is $P_{j,n}$, the algorithm processes the entry as follows: If the designated switch D_j in the entry is the same as Di then the entry is skipped (483). Otherwise the entry indicates there is a layer-2 link between D_i and D_j using ports $P_{i,m}$ and $P_{j.n}$ (484). The port numbers $P_{i,m}$ and $P_{j.n}$ thus identified are mapped to the interface IDs of the link by locating the dotldStpPortTable MIB entry at each device that matches each the device's port number. That is to say, the entries for ports $P_{i,m}$ and $P_{j,n}$ in the dotldStpPortTable MIBs of D_i and D_j, respectively, provide the ifIndex (485) values $I_{i,m}$ and $I_{j,n}$ that are recorded by the algorithm to identify the particular layer 2 link from D_i to D_j. Each entry is processed in this same manner until all of the layer-2 links are identified. The set of identified links, along with the layer 2 devices already identified earlier, comprise the output of the layer-2 topology analysis algorithm.

The concept of "identifying a port as an uplink port if said number of MAC addresses counted exceeds a predetermined number" does not appear in these paragraphs.

In view of this, the claim 2 is not taught or suggested since the concepts thereof are missing from Bearden et al. Haneda adds nothing that would provide the missing concept.

Therefore, it is respectfully submitted that the Examiner's application of Haneda (US 2002/0167914A1) in combination with in view of Bearden et al (US 2003/0086425A1) would not result in teaching or suggestion of applicants' claimed invention of claim 9.

New claims 3 and 4 are added. These claims are also believed to be allowable.

In light of the above noted amendments and remarks, this application is believed in condition for allowance and notice thereof is respectfully solicited. The Examiner is asked to contact applicant's attorney at 503-224-0115 if there are any questions.

It is believed that no further fees are due with this filing or that the required fees are being submitted herewith. However, if additional fees are required to keep the application pending, please charge deposit account 503036. If fee refund is owed, please refund to deposit account 503036.

Respectfully submitted,

James H. Walters, Reg. No. 35,731

Customer number 802
patenttm.us
P.O. Box 82788
Portland, Oregon 97282-0788 US
(503) 224-0115
DOCKET: F-370

Certification of Electronic Transmission

I hereby certify that this correspondence is being electronically transmitted to the Patent and Trademark Office via the EFS system on this July 23, 2007.